Doc ID: 6610955

RG 84
Box 1

NND 857560

~~TOP SECRET~~

November 24, 1944

I have read the underlying memorandum dated November 23, 1944 prepared by Mr. Paavo Carlson and Mr. Paul E. Goldsberry with respect to their recent conferences with the Finnish Black Chamber experts Pale, and Loimaranta, and find myself in general agreement with their account of what was said at these meetings.

I should like to emphasize, however, the pains taken to impress upon these Finns that we were interested only in information bearing upon the security of American communications or upon the prosecution of the war. At no time did we receive any Russian code material nor did we ask for any from the Finns. We did ascertain from them, however, that their collaboration with the Germans extended to probably a complete exchange of information on Russian codes.

Regarding the security of the strip cypher as now used the underlying memorandum, in my opinion, understates the degree to which the Finns claimed and demonstrated that they had progressed in breaking the system. Mr. Loimaranta demonstrated a complete knowledge of the channel elimination method. He also demonstrated that they did not have to rely upon a given mathematical volume of material to break the strip system: security violations on our part nearly always relieved them of the necessity of resorting to purely mathematical processes. Hence to my mind the inherent mathematical aspects of the strip system even in its present form are far from a reliable guide to the real security of the system. The Finns' own regard ~~with~~ for the system was well brought out, in my opinion, by their almost frantic request for a promise from us that under no circumstances would we send any messages regarding their contacts with us in the strip system.

W Randolph Higgs

Approved for Release by NSA on 01-12-2018, MDR Case # 101774

~~TOP SECRET~~

Doc ID: 6610955

~~TOP SECRET~~

November 23, 1944

November 16. Met at 11 a.m., at secret place. Tikander, Higgs, Lt. Snellman, and Capt. Pale. Higgs stated that purpose was to find out regarding State codes and any information which may be helpful to prosecution of war. Understood by Snellman and Pale. Snellman speaks no English. Pale does. Pale is probably Finn top man on Russian military codes. Insurance mathematician before war. Been crypto since December 1931. Pale stated he knew little of American diplomatic code but was expert on Russian. Further conversation developed he knew of our systems and methods of breaking. Stated we used book codes (G and Br?) superimposed book codes (ABC) and strip. Called strip by name. Stated that 6 months traffic in an unenciphered book code was enough to reconstruct a book. Stated enciphered code was difficult to solve. Re. strip. Stated that our weakness was in using same strip too long at once place and then using same strip for another post for direct communications. Spoke of lateral or intercommunication system. After reconstruction of set of strips by using same numerical key message is easily readable. Knew nothing re. channel elimination and stated we had probably changed strips late 1943 or early 1944. Thought that Finn (American section) had not made progress on strip traffic since December 1943. We asked re. machines. i.e., enigma. Stated very good and hard to break. Went on to say that Germans had a bigger and modified machine employing set of 6 or 9 wheels whereby you type as on a typewriter and the wheels turning would mix the text and is then printed in code on a tape. Has been and used that machine and states it is very good. Russian diplomatic codes are unbreakable - said they used a block of cipher groups and enciphered plain text only once on each group. Russian military and naval codes are numerical codes and ciphers which they use similar to strips by sliding and Finns read easily. They also use the additive and subtractive systems. Said he had been to Berlin and believes that Germans read some not all of our diplomatic codes. Said that they were not as adept as Finns. Does not think they read American military or naval codes, but believes they spend a great deal of time on British naval codes and with some success. We asked if Finns worked on Jap codes. He said no. "Too far away to be of interest". All traffic obtained through intercept. Helsinki traffic through cable office. Stated

Mr.

~~SECRET~~

oc ID: 6610955

TOP SECRET

Mr. Aalto would come over soon as possible. Mr. Aalto expert on American diplomatic codes. Meet again at 3 on Nov. 18, at secret place. Capt. Pale stated that collaboration with Germany consisted of exchange of information regarding Russia. Just enough to be an ally. Stated you have to "give a little and take a little".

Capt. Pale--about 40-45, small stature, very friendly and proud of his efforts, not boastful or braggart. Cryptanalyst on Russian military codes. Mathematician for Finn Insurance Company prior to war. Spoke very openly and did not try to hide anything. Speaks good English but apologized for lack of English stating he was in London last in 1933 and had used English very little since then.

Lt. Snellman--about 25-30. Liaison between OSS and Finn M.I.D. Six feet, medium build. Speaks no English. Pleasing personality. Made no comments. Previously explained enigma.

November 18. 3:30 - 5 p.m. Capt. Pale arrived alone saying that Snellman had been recalled and that he, Pale, had planned not to come but couldn't contact Tikander. Stated that Aalto would be unable to come inasmuch as he was now on a civilian status and couldn't obtain passport. This also applies to all others who m ght be of assistance to us, namely the American experts. Only one left in Sweden is Turkish expert, who we will meet Tuesday evening. He suggested that we go to Helsinki, where we could see Halmaa, Hendrickson, Aalto and any others who m ght be of assistance. Unable to do so, Seemed to be more hesitant than previously. We asked if cooperation with Japs which he emphatically denied saying Japs had asked for but obtained no information from Finns. Reiterated cooperation with Germans and stated Germans had furnished large volume of American traffic. He visited Lützen in East Prussia for five days some time ago, where Germans maintained b. c. for Russian traffic (no other). Now moved back. Stated German headquarters (very large) for b.c. was "south of Berlin" where great bulk of work is done. It is believed that his statement regarding the cooperation with Germany is enough to consider that Germans were also reading traffic. Lützen had about 300 persons and traffic they were unable to break was sent back to headquarters south of Berlin for analysis. He volunteered the information that all naval codes could be broken inasmuch as all traffic must be lateral and no point to point traffic and that volume would soon be obtained. Reaffirmed that machine was very good. O.T.P. is best. Said that stereotype greatly helps. Still says that our codes were broken through analysis

but

TOP SECRET

Doc ID: 6610955

TOP SECRET

but in his conversations he has stated that they have Russian, Turkish code books, so it is reasonable to assume they have photostat of Great Britain A.C. This, of course, he denies.

He broached the subject of some of their (Finn) experts going to United States where their analytical ability could be put to use. Stated that he (Pale) as a civilian would soon have to do something and preferred not to start in Sweden. When asked who would be available said, "only a few". Stated Finn b.c. were breaking Russian, Turkish, Rumanian, Jugoslav, and Vatican, as well as American. No attempt on German. Stated Germans were breaking British naval codes, he thought. Stated Finns had liaison officer at Lützen and Germans had man in Finn b.c. Meet again Tuesday evening, at 7 pm. November 21.

November 21. 7-10 p.m. Capt. Pale arrived with Mr. Kalevi Loimaranta, also an expert on codes and ciphers. In 1939 he was a mathematical student in the University. In the Army 1939 to December 1941, when Finn b.c. was enlarged. Worked on Russian, American, and Turkish ciphers. He is 26 years old. Stated the section that worked on American codes was composed of 10 or 12 people. Entire organization 1,000-1,200 of which greater part worked on Russian military and naval codes with such success that they were able to break a new code within two weeks after its first appearance. With help of Germans they were able to obtain large volume of traffic. At the armistice they still had large bins of unprocessed traffic, some of which they kept but large part was destroyed. Loimaranta worked in American section about 1½ years. He speaks no English so his statements were translated. We asked how they obtained names of codes and designations of strips. Through acknowledgement by code telegrams. We then asked how they broke our strip cipher. This, he said, was done largely through stereotyped beginnings and endings after having obtained a volume of traffic. Stated that we used 30 strips up until this year. Since that time they suspect that we only use 25 which we did by withdrawing 5 of the original 30. They suspect that the indicator designates the strips to be withdrawn. Stated that since January 1944 they have done little work on American codes and cipher. Once they had obtained sufficient traffic for analytical purposes and were able to reconstruct one set of strips, then through security violations, i.e., stereotyped phraseology, beginnings, etc., they were able to reconstruct new sets. They would obtain texts of meetings in Helsinki and wait for message reporting that meeting, then fit the two together and reconstruct strip systems. Stated that our using same set of strips at different places also made their work easier. Our use of the same numerical key also helped them. They used I B M machinery in their analytical processes and employ very few women. Only card punchers.

Prefer

SECRET

Doc ID: 6610955

Prefer men under 30 years. Their method of breaking codes is based on volume of traffic obtained. Believe that in a year they could reconstruct a large part code of 100,000 groups. They reiterated their belief that machine cipher the nearest thing to unbreakable with the exception of O.T.P. Pale stated that he had constructed such a cipher (O.T.P.) for Finn diplomatic messages. It may now be in use between Helsinki and Tokyo. Stated again that they had given no aid to Jap Attaché in Helsinki, nor had they received any assistance from them.

Conclusions: While they deny that they have obtained possession of Great Britain's A-B-C code books, it is believed that they may have obtained actual possession of the British and possibly others. They possess great knowledge of our S.C. system, i.e., construction and designation of alphabet sets; calendar keys and numerical sequences. They know that since December 1943 we have changed the arrangement of strips in the device and strongly suspect that the method is elimination. They know nothing of our use of machines, mechanical devices or O.T.P. There is some contradiction as to their having broken any military codes and they have not attempted to break naval codes.

Close cooperation existed between the Finnish black chamber and the Germans with respect to Russian military and naval codes. Germans obtained some assistance from the Finns on American diplomatic codes and in return the Germans furnished large volume of traffic to be processed by the Finns. In view of the collaboration that existed between the Finns it is believed that the Japs may have obtained some assistance from the Germans concerning our codes and ciphers, but none directly from Finns even though they (the Japs) asked for cooperation. It is believed that the Germans had a very good knowledge of our S.C. as it existed prior to December 1943 and it is possible that they now possess information regarding the present channel elimination method. Further, it is believed that Germans have had some success on breaking British naval codes.

Drafting offices in the Department and in the field should be instructed as to the danger of using stereotyped phraseology.

More careful study of crypto security practices should be instituted in the code room, especially for the benefit of F.S. clerks, as well as new checks for code room.

W.F.P.C.